

Challenges of Unlicensed Wi-Fi Deployments: A Practical Guide for Cable Operators

Overview

Major Wi-Fi deployments are in progress in most of the cable operator community. These are guided by different business models, but all rely on the operator advantages with right of way, power, and backhaul. These advantages are countered by the unlicensed nature of Wi-Fi. This document will provide an overview of the physical and MAC layer features that allow Wi-Fi to work in challenging environments. Other topics covered are guidelines for deployment strategies, monitoring, and troubleshooting.

Introduction

The increase in demand for Wi-Fi Internet access is growing at a pace faster than that of traditional wired and cellular Internet. The fact that every portable device has some type of Wi-Fi client capability promotes this growth. The positive side is that service providers don't need to subsidize client devices. The negative side is the bring-your-own-device (BYOD) mentality. This not only introduces support challenges but adds to deployment engineering challenges.

The accelerated growth of Wi-Fi has also created higher ambient noise and interference levels in urban and suburban areas. This added noise and interference, although somewhat manageable with the 802.11 MAC layer, does reduce the likelihood of predictable service levels.

Wireless RF

Propagation

There is a very good understanding of RF principles in the cable community. The basic concepts of receive signal, transmit signal, and signal to noise ratio (SNR) are well understood by plant construction and operations personnel. The modulation schemes used in Wi-Fi are also similar to the ones used in a DOCSIS plant.

The basic wireless signal has four major factors that affect propagation: absorption, reflection, refraction, and diffraction.

The most detrimental of these is absorption. Absorption is to wireless RF as poor-quality coaxial cable is to a DOCSIS plant. Absorption can be caused by the air we breathe in the form of oxygen and water vapor. Other natural absorption can be caused by living things, including people and foliage. You will, for example, lose significant signal if you are in a crowd of people at a concert or at a park surrounded by trees. Formulas are available to calculate free space path loss, but a rule of thumb is an average loss of 104 dBm at 2.4 GHz over one mile. You can also expect a loss or gain of 6 dBm as you double or halve your distance. The typical loss at 1/8 mile or 660 feet would be approximately -86 dBm.

The next effect is reflection. The magnetic wave is reflected from metallic and other reflective surfaces. This can be your friend or enemy. When you receive a signal without a direct line of sight, then you are benefitting from reflection. There are situations when excessive reflection, such as over water, chain-link fences, and other long surfaces, can cause so much signal distortion that you can have fades and nulls in the received signals. The other thing to note about reflection is that it can also be caused by surfaces that would normally absorb but have a low angle of attack. An example is when you try to cover a strip mall and cannot place the access points directly in front.

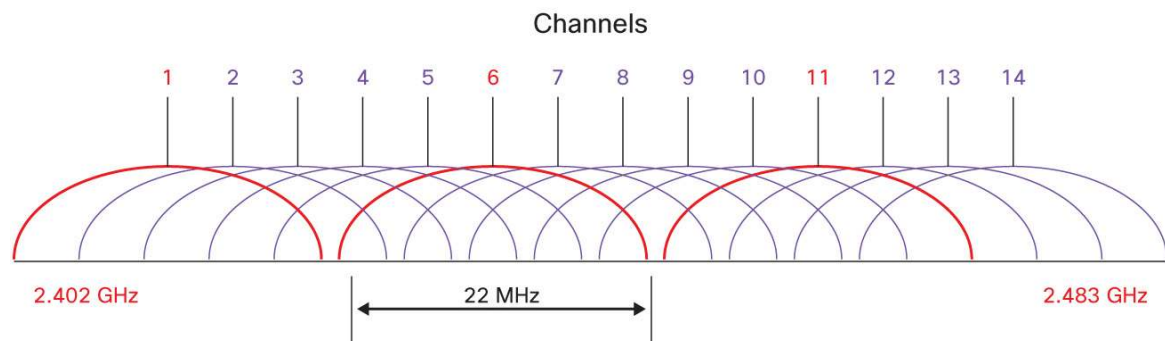
The last two effects are diffraction and refraction. These are less noticeable, but some examples are solar coated glass, hot summer days, and proximity of access points to telephone poles and other strand-mounted assets.

The net result is that disruption of the radio transmission produces a corresponding reduction in distance and signal quality. This reduction is directly related to obstruction in the Fresnel zone. This is the midpoint signal energy required to drive the signal over the long distance. Obstruction determines whether the link is defined as line of sight (LOS), which is 60 percent or more Fresnel clearance, near-LOS (near line of sight), which less than 60 percent, or non-LOS, which is a fully obstructed signal. The differences determine whether a model can determine coverage or field measurements need to be performed.

Frequencies

The current access point technologies use one of two spectrum bands. These are channels in the 2.4 and 5 GHz industrial scientific and medical (ISM) bands. They are unlicensed in the U.S. and operate under FCC Part 15 rules. These rules govern the transmit power and channel width and modulation. The most common of these is the 2.4 GHz band. This is used by the 802.11b/g and 11n devices. There are 11 channels but they are 20 MHz wide with a 1 MHz guard band on each side, so there are ultimately only three that don't overlap: channels 1, 6, and 11 (see Figure 1).

Figure 1. U.S. 2.4 GHz Channel Plan

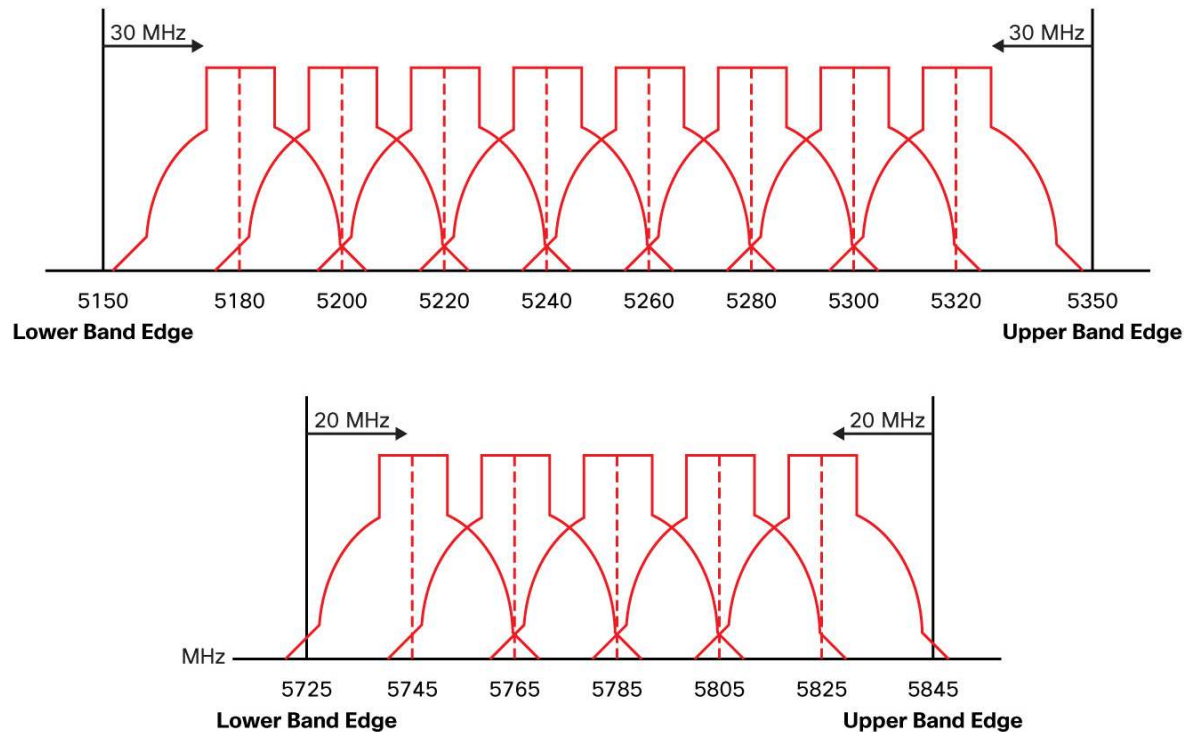


This provides 60 MHz of spectrum, but in congested areas it can be very busy. The band is also shared by other technologies such as Bluetooth, cordless phones, wireless video cameras, and microwave ovens. The 2.4 GHz band is the most populated by Wi-Fi and carries for longer distances from a propagation perspective.

The 5 GHz bands provide up to 21 channels in the U.S. (Figure 2). The channels are spread in three groups: UNII-1, UNII-2 and UNII-3. They have different rules regarding use and power but are generally available. The UNII-1 band is reserved for indoor use only. The UNII-2 band has specific restrictions with respect to radar interference. There are currently fewer ISM consumer devices in these bands, but they do exist. The propagation at 5 GHz is reduced due to the higher frequency.

This reduction, however, is countered by the lower noise in these bands. The result is that outdoor Wi-Fi can have similar usable distance on both 2.4 and 5 GHz. The newer consumer devices coming into the market support 5 GHz, including Samsung and Apple smartphones and the iPad.

Figure 2. U.S. 5 GHz Channel Plan



802.11 Modulation Techniques

The 802.11 standard makes provisions for the use of several different modulation techniques to encode the transmitted data. These modulation techniques are used to enhance the probability of the receiver correctly receiving the data, thus reducing the need for retransmissions. They were originally intended for military use to provide a mechanism to transmit data while being jammed. The techniques vary in their complexities and robustness to RF signal propagation impairments.

The modulation techniques are direct sequence spread spectrum (DSSS) and orthogonal frequency division multiplexing (OFDM). The DSSS approach used in 802.11b involves encoding redundant information into the RF signal. Every data bit is expanded to a string of chips called a chipping sequence or Barker sequence. The chipping rate, as mandated by the U.S. FCC, is 10 chips at the 1- and 2-Mbps rates and 8 chips at the 11-Mbps rate. So at 11 Mbps, 8 bits are transmitted for every one bit of data. The chipping sequence is transmitted in parallel across the spread spectrum frequency channel. The OFDM used in 802.11a, 802.11g, and 802.11n data transmissions offers greater performance than the older direct-sequence systems. In the OFDM system, each tone is orthogonal to the adjacent tones and therefore does not require the frequency guard band needed for direct sequence. This guard band lowers the bandwidth efficiency and wastes up to 50 percent of the available bandwidth. Because OFDM is composed of many narrow-band tones, narrow-band interference degrades only a small portion of the signal, with little or no effect on the remainder of the frequency components (see Table 1).

Table 1. 802.11a/g/n Modulations

11a/g MCS	Modulation	Wireless Throughput
6 Mb/s	BPSK 1/2	6 Mb/s
9 Mb/s	BPSK 3/4	9 Mb/s
12 Mb/s	QPSK 1/2	12 Mb/s
18 Mb/s	QPSK 3/4	18 Mb/s
24 Mb/s	16QAM 1/2	24 Mb/s
36 Mb/s	16QAM 3/4	36 Mb/s
48 Mb/s	64QAM 2/3	48 Mb/s
54 Mb/s	64QAM 3/4	54 Mb/s

# of Spatial Streams	11n MCS	Modulation	Min SNR (dB)	Wireless Throughput
1	MCS 0	BPSK 1/2	5	7 2/9
1	MCS 1	QPSK 1/2	7	14 4/9
1	MCS 2	QPSK 3/4	9	21 2/3
1	MCS 3	16QAM 1/2	13	28 8/9
1	MCS 4	16QAM 3/4	17	43 1/3
1	MCS 5	64QAM 2/3	20	57 7/9
1	MCS 6	64QAM 3/4	22	65
1	MCS 7	64QAM 5/6	23	72 2/9
2	MCS 8	BPSK 1/2	5	14 4/9
2	MCS 9	QPSK 1/2	7	28 8/9
2	MCS 10	QPSK 3/4	9	43 1/3
2	MCS 11	16QAM 1/2	13	57 7/9
2	MCS 12	16QAM 3/4	17	86 2/3
2	MCS 13	64QAM 2/3	20	115 5/9
2	MCS 14	64QAM 3/4	22	130
2	MCS 15	64QAM 5/6	23	144 4/9

The 802.11 protocol allows for retransmissions, which are shifted to more robust modulation. The transmissions do get through, but the retransmissions cause some latency and will lower overall throughput. You should maintain the appropriate SNR for the given modulation, but you want to stay in the double-digit range, and a 20 dBm SNR is preferred. This can be a challenge in very noisy areas that can have noise floors in the mid-80s. You would need signal levels at -65 dBm or better for maximum throughput.

802.11 MAC Layer

The 802.11 MAC layer is based on Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA). The two most common frames are distributed coordination function (DCF) and enhanced DCF (EDCF) frames (see Figures 3 and 4). They are similar with the difference that EDCF allows for some concept of statistical quality of service (QoS).

Figure 3. DCF Frame

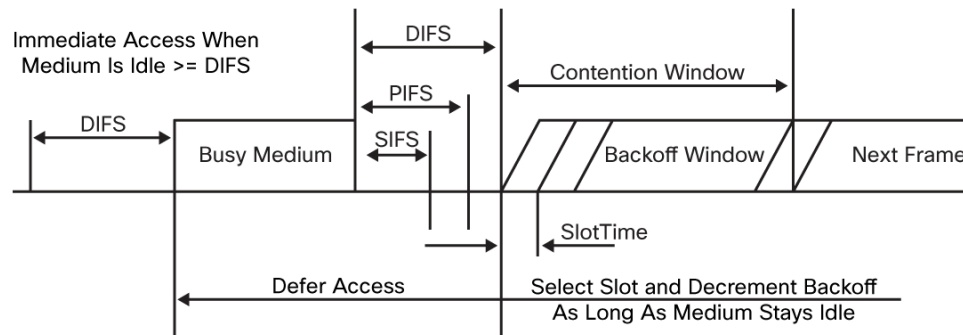
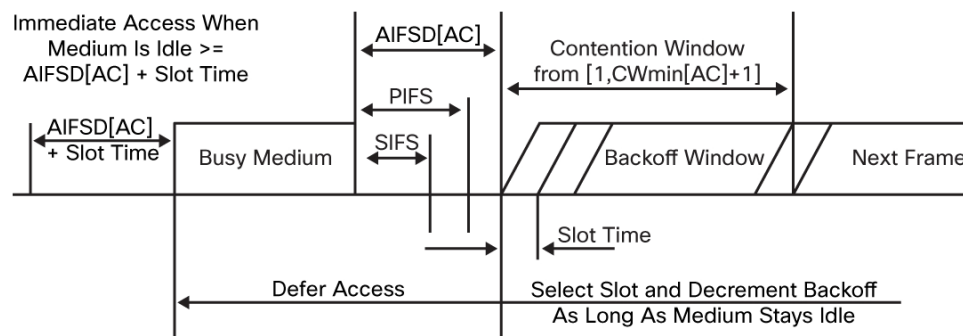


Figure 4. EDCF Frame



CSMA/CA

Basic media access starts with the device ready to transmit awaiting a DCF interframe space (DIFS) for clear channel. The clear channel assessment (CCA) varies by manufacturer. Some devices just look for a certain energy level and others look for some type of carrier. The CCA signal levels also vary by manufacturer. There are instances when there is so much noise and co-channel interference that even a well-designed network will be muted. The other problem that can occur in a CSMA method is a hidden node. This can be a problem when trying to create large cells or trying to cover indoor locations from outdoors. The clients can communicate with access points but are too far apart to hear each other. When the spectrum is extremely bad the Wi-Fi devices can switch to a point coordination function (PCF) and implement a Ready To Send (RTS) and Clear To Send (CTS) scheme.

802.11 Frames

Once the CCA is completed, the device will transmit and all devices will await a short interframe space (SIFS) for an acknowledgment to be sent. These delays are what contribute to the reduction in wireless throughput. In 802.11a/g these are roughly 50 percent of wireless speeds. The packets that are not acknowledged are retransmitted until the retransmit limit is reached or the packet goes through. The EDCF allows for variable random backoff to create statistical QoS for critical applications.

802.11 Messaging

The most common 802.11 messages are the management frames. The most visible are the beacons. These are regular messages sent from the access point that advertise the service set identifier (SSID) and the broadcast MAC address (BSSID). The beacon also advertises the enabled speeds and authentication and encryption methods available for that SSID. The beacon is used for clients with passive association mechanisms and also as a keepalive message for clients to detect loss of the access point.

The broadcasts are sent every 100 ms for each configured SSID, so one must consider each access point will generate 10 broadcasts per second per SSID. The other consideration is that management frames are sent at the lowest mandatory data rate. The 802.11 management frames are not currently signed and are therefore subject to spoofing and potential denial of service attacks.

Deployment Strategies

The deployment strategy for a cable operator varies by geography. Some areas have abundant overhead plant and others have only underground plant. Other considerations include the target end-customer data rates and application types being deployed and supported client devices. Deployments also may vary based on the noise and co-channel interference in any given area.

Client Devices

The client device is the least common denominator in Wi-Fi deployments. Among the essential components of Wi-Fi communication, the client device type will have the most influence on range and throughput (for example, a device may have limited or no antenna gain and low transmit power, two factors that have a direct relationship to throughput and range). Client devices are also responsible for deciding what access point to join and when to roam.

Supported Applications

Application requirements also dictate deployment metrics. The best applications are ones that can operate on available or variable bitrates. These include email, web surfing, and buffered video. You have to deliver much higher signal levels to support more demanding applications such as voice and streaming video.

Client Density

The average access point can associate more than 200 wireless users. This association count is only one of several factors that contribute to association counts. The only workable solution to high client density is to deploy more access points at lower transmit power with more directional antennae. The best wireless experience results from keeping average associations to between 20-50 users. You must also consider the backhaul and upstream infrastructure for the next level of bottlenecks.

Supported Data Rates

Supported data rates have the second largest influence on range, after free space loss, reviewed earlier. The solution to this puzzle is indicated by the sample receive signal levels shown in Table 2.

Table 2. Sample Receive Sensitivity

2.4 GHz	5GHz
802.11g (non HT20) -92 dBm @ 6 Mb/s -92 dBm @ 9 Mb/s -92 dBm @ 12 Mb/s -90 dBm @ 18 Mb/s -86 dBm @ 24 Mb/s -84 dBm @ 36 Mb/s -79 dBm @ 48 Mb/s -78 dBm @ 54 Mb/s	802.11n (HT20) -93 dBm @ MCS0 -91 dBm @ MCS1 -89 dBm @ MCS2 -86 dBm @ MCS3 -83 dBm @ MCS4 -78 dBm @ MCS5 -77 dBm @ MCS6 -75 dBm @ MCS7 -87 dBm @ MCS8 -87 dBm @ MCS9 -85 dBm @ MCS10 -83 dBm @ MCS11 -79 dBm @ MCS12 -75 dBm @ MCS13 -73 dBm @ MCS14 -72 dBm @ MCS15
802.11n (HT20) -92 dBm @ MCS0 -90 dBm @ MCS1 -88 dBm @ MCS2 -85 dBm @ MCS3 -82 dBm @ MCS4 -77 dBm @ MCS5 -76 dBm @ MCS6 -74 dBm @ MCS7 -92 dBm @ MCS8 -90 dBm @ MCS9 -87 dBm @ MCS10 -85 dBm @ MCS11 -82 dBm @ MCS12 -77 dBm @ MCS13 -75 dBm @ MCS14 -74 dBm @ MCS15	802.11n (HT40) -91 dBm @ MCS0 -89 dBm @ MCS1 -87 dBm @ MCS2 -83 dBm @ MCS3 -80 dBm @ MCS4 -75 dBm @ MCS5 -74 dBm @ MCS6 -72 dBm @ MCS7 -86 dBm @ MCS8 -85 dBm @ MCS9 -84 dBm @ MCS10 -80 dBm @ MCS11 -77 dBm @ MCS12 -72 dBm @ MCS13 -71 dBm @ MCS14 -70 dBm @ MCS15

The signal level should also include a 5 to 10 dBm fade margin as well as a 20 dBm SNR. The target signal level to achieve a modulation and coding scheme (MCS) 15 data rate of 144 Mbps should have a receive signal of -64 to -69 dBm. These levels should also provide a 20 dBm SNR in very noisy areas. The typical client may have a transmit power of 14 dBm. The average smartphone would have very little if any antenna gain and an access point would have between 2 and 5 dBi of gain. This would yield a system gain of 16 to 19 dBm. The target signal level for MCS15 is -64 dBm. The signal level minus the system gain of 16 dBm allows us to lose 80 dBm over free space, or about 325 feet.

Site Planning

Site selection is determined by several factors. The first is the coverage target. The business decision to cover an outdoor location or indoor venue is the first step in a deployment process. The use of aerial plant provides power, backhaul, and mounting locations. This has a very low cost of entry but may yield a best-effort deployment. You can generally use wireless RF planning tools to visualize the coverage. In the areas where no aerial plant is available, one alternative is a vault or pedestal mount. These mounts will have a lower cell size because they have more ground obstruction. The other alternative is an indoor unit in the target venue or a nearby venue.

Monitoring

The day-two operations of a Wi-Fi network will vary based on the access point technology. Once the access point is deployed, you can use several metrics to determine the health of a network. The basic gauge is the number of associations. The next is network utilization. You can add session duration, but public outdoor networks tend to have drive-by users that skew session lengths. You have to consider other factors while trending these gauges, including weather, holidays, and significant news events.

RF Statistics

The monitoring of FCS errors, retries, and RTS retries will be beneficial in detecting areas of interference. You may also have access to the channel and power decisions the access points are making to further identify problem areas. The other statistic to look at is average data rate. If the access point is spending more time at the lower data rates, you may be seeing interference or clients that are too far away.

Interference and Non-Wi-Fi Interference (Noise)

In the Wi-Fi world, anything that looks like Wi-Fi is considered an interferer and the rest is considered noise. The major difference is that something that looks like a Wi-Fi carrier despite the signal level will suppress transmissions because of CSMA/CA. If this is just noise then there is generally a CCA threshold that must be reached before suppressing transmits. In some architectures the access points may adjust channel and power levels dynamically to avoid environmental or neighbor interference.

Security

There are several security risks even when operating an open Wi-Fi network. The majority involve spoofing. You may have someone spoof your SSID or even your access point MAC. The other security risks include spoofing of client MAC addresses, bogus management frames, and Wi-Fi jammers.

Troubleshooting

The main consideration in trying to resolve Wi-Fi issues is that several layers interact to produce a Wi-Fi session. If any of these layers are experiencing an issue then the net result is the same: "the wireless doesn't work." The user doesn't necessarily realize that the Wi-Fi is working fine but the DHCP server or web portal may be broken. You need to break the issue down to the various layers in the service offering. The layers include physical, MAC, IP services, and Internet.

Physical Problems

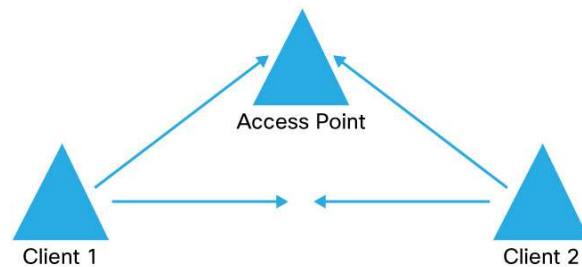
These problems should be fairly easy to track. You can verify whether there are other users on the access point in question and whether the user sees the SSID. You can go on to investigate whether the client is making any attempt to connect. In a typical network you have an open authentication, so there are fewer reasons why a client cannot communicate. You also have some reassurance that Wi-Fi certified products have been tested at this basic level.

The manifestations of physical RF issues are FCS errors, excessive retries, long retries, and low throughput. You may also notice RTS retries. The worst scenario would be the presence of low throughput with little or no RTS and long retries. This usually indicates significant noise in the spectrum.

MAC Layer Issues

In the MAC layer we see issues involving CCA and hidden nodes (Figure 5). The busier the channel is from co-channel and non-Wi-Fi interference, the lower the throughput, and you would notice very few retries and no RTS retries. When you have hidden-node problems, you will see lower throughput and many retries.

Figure 5. Hidden Node



IP Services

The IP services layer includes DHCP, DNS, and NAT. In the event that any one of these does not function properly, most client devices will not complete the association process.

Conclusion

The concept of using Wi-Fi as a broadband access technology is viable. There are challenges that relate to coexistence with other nonlicensed implementations. The physical layer of Wi-Fi provides several mechanisms to cope with significant interference. You need to consider what is possible with Wi-Fi and offerings that are consistent with the network design. The coverage of outdoor venues from cable assets should work in the majority of instances. The attempt to cover indoor locations from outdoor access points will yield mixed results. There will be at least first-wall penetration. The better solution would be to provide a value add-on for the venue and place indoor access points at those locations. Several U.S. cable operators have deployed thousands of access points and have a good working knowledge of these practices.

For More Information

"IEEE 802.11e Contention-Based Channel Access (EDCF) Performance Evaluation," by Sunghyun Choi, Javier del Prado, Sai Shankar, and Stefan Mangold

Wi-Fi (802.11) Network Handbook, by Neil P. Reid, and Ron Seide




Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

 Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA

C11-716080-00 11/12